PUBLIC OFFER

On Provision of Payment Services through the Octomobile Mobile Application

By this Public Offer On Provision of Payment Services through the Octomobile Mobile Application (the Offer), Octobank Joint Stock Company (the **Bank**) **offers** an individual, including the Bank's Client (the **User**), to conclude a payment services agreement (the **Agreement**) on the terms set out below.

In accordance with articles 364, 367, 369 and 370 of the Civil Code of the Republic of Uzbekistan, this document is an official public offering of the Bank.

1. TERMS AND DEFINITIONS

Authorization – a procedure for requesting and obtaining permission by the Bank to conduct a Transaction.

Acceptance of the Offer – the complete and unconditional acceptance by the User of the terms of this Offer by performing Implicative Actions.

Authentication Data – unique User data used to access the Personal Account and confirm operations: login, password, Biometric Data, as well as Verification Codes.

Biometric Identification (Biometrics) – a procedure for identifying a User in a Mobile Application based on their physiological and biological characteristics (face recognition, fingerprint, and other methods), including using remote identification systems.

Bank – Octobank Joint–Stock Company, operating under a License from the Central Bank of the Republic of Uzbekistan and a provider of payment services.

Bank's internal regulations – a set of local acts, rules, instructions and procedures independently approved by the Bank that regulate internal technological processes, the procedure for setting limits, identification procedures (KYC), internal control rules (including AML/CFT), as well as information security and cybersecurity regimes.

Deposit account – a User's bank account opened at a Bank, intended for accounting and performing transactions with funds.

Card – a bank card of the payment systems UZCARD, HUMO, VISA, MASTERCARD and other payment systems issued by a Bank or a Third–Party Bank, linked by the User to the Mobile Application for making Transactions.

Implicative Actions – actions of the User expressing its will to conclude a Contract or perform an Transaction (registration in the Mobile Application, entering a verification code, taking Biometrics, pressing buttons that initiate the Transaction). According to Article 370 of the Civil Code of the Republic of Uzbekistan, such actions are equivalent to Acceptance of the Offer.

Commission – the Bank's remuneration for the provision of Services provided for in the Tariffs.

Personal Account – a personalized section of the Mobile Application, protected by Authentication Data, intended for remote control of banking services, Transactions and access to the User's transaction history.

Mobile Application (Octomobile Application) – a specialized software that is a set of Bank software installed on a Mobile Device in the legal possession of the User, the functionality and version of the operating system of which support the installation and correct operation of the Mobile Application.

Mobile Device – a mobile phone and/or tablet computer, and/or
a portable computer and/or other device of the User, the software environment of which allows using the full functionality of the Mobile Application to receive the Bank's Services as part of this Offer.

Transaction – any banking Transaction involving the transfer of funds, payment for goods (works, services) in the RSO, replenishment of accounts, including payment of the Bank's commission for Services provided in accordance with the Bank's Tariffs and other operations performed by the User through a Mobile Application.

Payment Window – an interface in the Mobile Application that displays the Transaction parameters and conditions before the final confirmation.

User (Client) – an individual who is a Cardholder and/or account holder who has concluded an Agreement with the Bank by Accepting the Offer.
Verification Code (OTP code) – a unique sequence of characters (one-time password) sent by the Bank to the User (SMS/Push) to confirm actions in the Application.
Order – an instruction from the User to the Bank to perform a Transaction (payment or transfer), generated in the Mobile Application and confirmed by Authentication Data.
Third–Party Bank – a commercial bank or other credit institution of the Republic of Uzbekistan (except for Octobank JSC) that has the appropriate license from the Central Bank of the Republic of Uzbekistan to operate and the right to issue bank cards.
Card Account – a bank account opened with the issuing bank to carry out transactions using the Card.
Tariffs – the Bank's commission fees posted on the Bank's Website and in the Mobile Application.
Token – a unique digital identifier of a Card generated by the tokenization platforms of international or national payment systems and linked to a specific Mobile Device of the User for carrying out Transactions through a Digital Wallet.
RSO (retail and service outlet) – a legal entity or individual entrepreneur whose goods or services are paid for by the User through a Mobile Application.
Service – a payment service and related services provided by the Bank through the Octomobile Application.
Face ID / Touch ID – methods of Biometric identification and User authentication based on facial feature recognition (Face ID) or fingerprint (Touch ID). These technologies are used as a tool for accessing the Mobile Application and are recognized by the Parties as an analogue of the User's handwritten signature to confirm Orders for debiting funds.
MCC code (Merchant Category Code) – a four-digit code that classifies the type of RSO activity in the payment system.
Push Notification (Push) – a short electronic message that appears on the screen of the User's Mobile Device and is used by the Bank to inform the User.
Digital Wallet (Payment Service) – a software service provided by a third party (including Apple Pay, Google Pay / Google Wallet and others) that is installed on or supported by the User’s Mobile Device and enables the secure storage of a digital representation of the Card (Token) and its use for contactless payments and transactions over the Internet.
Provisioning (Adding a Card) – a feature of the Mobile Application that allows the User to securely initiate the transfer of data relating to a Card issued by the Bank to a Digital Wallet on the Mobile Device, for the creation and activation of a Token without manually entering the Card details.
QR code – a standardized matrix barcode that allows for initiating a payment in favor of a RSO by scanning it through the Mobile Application using any available User Card. The QR code can be:

— static (containing unchanged payment details of the RSO, while the Transaction amount is entered by the User independently in the Mobile Application);
— dynamic (generated by the RSO separately for each Transaction, containing a unique identifier, the amount of the Transaction and having a limited validity period).

SMS (Short Message Service) – a short text message service that allows the Bank to send information about Transactions and changes in Tariffs/Offer to the User's confirmed mobile phone number, as well as one-time Verification Codes.

2. SUBJECT MATTER OF THE AGREEMENT

2.1. The subject matter of this Agreement is the provision by the Bank to the User of payment and related services through the Mobile Application on the terms set out in this Offer, including the technical capability to link Cards issued by the Bank to Digital Wallets and to perform other actions supported by the Mobile Application.
2.2. The Bank provides technological and informational interaction between the User, payment systems and payment recipients (RSOs) for real-time Transactions.

2.3. The Bank provides Services in accordance with the requirements of the laws of the Republic of Uzbekistan, the Rules of payment systems and Internal Regulations of the Bank.

2.4. The specific list of available Transactions, the functionality of the Mobile Application, and restrictions (limits) are set by the Bank independently and can be changed unilaterally.

3. PROCEDURE AND CONDITIONS OF ACCEPTANCE OF THE OFFER

3.1. This Agreement is concluded by acceptance (Acceptance) by the User of the terms of this Offer in accordance with Articles 367 and 370 of the Civil Code of the Republic of Uzbekistan. Acceptance of the terms of the Offer means the User's full and unconditional agreement with all its provisions, including Tariffs and Internal Regulations of the Bank, without any exceptions or reservations.

3.2. The User accepts the Offer by performing the following Specific actions in the Mobile Application:

3.2.1. Understanding the text of the Offer in the Application interface.

3.2.2. Completing the registration or authorization procedure using a mobile phone number.

3.2.3. Confirmation of registration/authorization by entering a one-time Verification Code (SMS/Push) sent by the Bank.

3.2.4. Biometric Identification (if provided by the functionality of the Application).

3.3. From the moment of performing any of the above actions, the Agreement is considered concluded in electronic form (equivalent to written form), acquires legal force and generates obligations for the Parties.

3.4. By accepting the Offer, the User confirms that it:

3.4.1. provided reliable personal and contact information;

3.4.2. fully understands the legal consequences of his actions.

4. GENERAL TERMS OF SERVICE PROVISION

4.1. The Bank provides Services only if it is technically possible to perform each specific Transaction in real time.

4.2. For the provision of Services, the Bank charges the User a Commission according to the Tariffs in force at the time of the Transaction.

4.3. The User gives its unconditional consent (acceptance) to debit the Commission without additional instructions at the time of the Transaction. The Commission is charged in excess of the amount of the main Transaction from the Card or Account from which the Transaction is performed.

4.4. If there is no amount on the Card or Account sufficient to carry out the Transaction and pay the full Commission, the Transaction will not be performed.

4.5. Transactions through the Mobile Application are carried out in the national currency of the Republic of Uzbekistan (SOUM), as well as in foreign currency within the available functionality.

4.6. In case of a mismatch of the Account/Card currency/, the User instructs the Bank to convert the funds in the following order:

4.6.1. For intrabank transactions (currency exchange within the App between their accounts) — at the exchange rate set by the Bank for exchange transactions in the Mobile App at the time of the Transaction.

4.6.2. When paying for goods and services (including in favor of foreign RSOs) — at the special rate of the Bank set for bank card transactions in payment systems on the date and time of processing the Transaction (debiting funds from the account). The User accepts and confirms that the specified exchange rate may differ from the conversion rate announced on the Bank's official website for other types of transactions.

4.7. The User has been notified and agrees that the date and time of the Transaction confirmation in the Mobile Application may not coincide with the date of the actual debit of funds from the account due to the regulations of payment systems. In this regard,

the resulting exchange rate difference (due to a change in the exchange rate at the time of processing the transaction by the processing center) is credited to the User's account and is not reimbursable by the Bank.

4.8. For safety and compliance with legal requirements (including AML/CFT), the Bank sets limits on the amount of Transactions (one-time, daily, monthly). The Bank has the right to change the limits unilaterally.

4.9. The Bank may not to execute the User's Order in the following cases:

4.9.1. When using Cards issued to accounts of legal entities or individual entrepreneurs (corporate cards).

4.9.2. In the absence of a positive Authorization from the issuing bank or payment system.

4.9.3. In the presence of arrests, blockages or other restrictions imposed by authorized state bodies on Accounts/User's cards.

4.9.4. If there is suspicion that the transaction is of a dubious nature or is carried out for the purpose of legalizing income from criminal activities, financing terrorism and proliferation of weapons of mass destruction or breaches the laws of the Republic of Uzbekistan.

4.9.5. In case of mismatch of Authentication Data or failure of Biometric identification.

4.9.6. In other cases stipulated by the laws of the Republic of Uzbekistan and/or Internal Regulations of the Bank.

4.10. All notifications about the successful or unsuccessful completion of the Transaction are sent to the User via the Mobile Application interface (Push notifications) and/or via SMS messages to a confirmed phone number.

4.11. The User may add Cards issued in its name from Third-Party Banks to the Mobile Application and perform Transactions for them (including cross-border transfers and payment for services using currency conversion). When performing such Transactions, the User instructs the Bank to send a request to debit funds to the issuing bank of the corresponding Card of a Third-Party Bank.

5. SERVICE PROVISION

5.1. The Service is provided on the basis of the User's electronic order generated in the Mobile Application.

5.2. To initiate a Transaction, the User selects the appropriate type of Service in the menu of the Mobile Application and fills in the necessary details in the Payment Window.

5.3. Until the Transaction is confirmed, the Bank displays the key parameters in the Payment Window: the amount of the Transaction, the amount of the Commission (if any), and the total amount to be debited.

5.4. The User shall independently verify the correctness of the entered data (recipient's card/account number, phone number, amount, etc.) before confirming the Transaction.

5.5. The order is confirmed by the User by entering a Verification Code (SMS/Push) and/or passing Biometric identification (Face ID/Touch ID), depending on the security settings and the type of the Transaction.

5.6. Entering the correct Verification Code received via SMS or Push notification, as well as successful authorization using Face ID or Touch ID, are recognized by the Parties as an unambiguous and indisputable confirmation of the User's will (analogous to a handwritten signature). From this moment on, the Order is considered accepted by the Bank for execution and cannot be revoked by the User.

5.7. After confirming the order, the Bank performs the Authorization procedure in real time.

5.8. In case of successful Authorization, the Transaction amount and the Commission amount are debited from the User's Account/Card.

5.9. If Authorization is not possible (no funds, incorrect banking details, technical failure on the side of Payment systems, etc.), the Bank informs the User about the refusal to perform the Transaction through the interface of the Mobile Application.

5.10. The Bank's obligations under this Agreement regarding the execution of the Transaction are considered to be fulfilled properly and in full in any of the following cases:

5.10.1. at the time of debiting funds from the User's Account/Card and sending the corresponding electronic confirmation (payment information) by the Bank to the address of the payment system or the recipient bank.

5.10.2. at the time of sending a notification to the User about the refusal of the Transaction (via the Mobile Application interface, SMS or Push notification) indicating the reason for the refusal, provided that the refusal is caused by circumstances beyond the control of the Bank or provided for by the terms of the Offer.

5.11. From the moment the result of the Transaction is recorded in the Bank's electronic logs, the Service for processing this particular User's order is considered to have been provided.

5.12. The Bank is not responsible for the timing of the subsequent transfer of funds to the recipient's account if the delay is caused by the actions of third-party banks or payment systems.

5.13. Confirmation of a successful Transaction is information indicating the details of the Transaction generated in the Mobile Application, which is available for viewing and saving in the Monitoring section.

5.14. When performing a Transaction by scanning a QR code, the Bank ensures that the following data is displayed in the Payment Window until the User confirms the Transaction:

5.14.1. name (trade name) of the RSO;

5.14.2. Transaction amount (filled in automatically for a dynamic QR code or entered manually by the User for a static QR code);

5.14.3. the amount of the Bank's Commission.

5.15. The User shall personally verify the correctness of all data displayed in the Payment Window before the actual confirmation of the Transaction. Confirmation of the Transaction (entering a code or Biometrics) after displaying the specified parameters is recognized as an irrevocable order from the User and confirmation of his consent to the amount, the details of the RSO and the commission.

5.16. Procedure for linking Cards to Digital Wallets through the Mobile Application:

5.16.1. The User has the right to initiate the addition of a Card issued by the Bank to a Digital Wallet using the dedicated feature in the Mobile Application interface.

5.16.2. The User’s pressing of the button to add a Card to a Digital Wallet and subsequent confirmation of the operation using the Mobile Application’s authentication methods (entry of the Verification Code (OTP), Face ID / Touch ID biometric authentication, or a passcode) shall be deemed by the Parties to constitute the User’s unconditional electronic instruction to issue the corresponding Token and acceptance of the Terms and Conditions for Tokenization and Use of Bank Cards in Digital Wallets (Appendix No. 2 to the Bank’s Public Offer on the Issuance and Servicing of Bank Cards).

5.16.3. The Bank shall ensure the creation and transmission of a cryptographic data package for creating the Token to the Mobile Device’s operating system and the Digital Wallet. The Bank may require additional verification or refuse to complete the addition of the Card to the Digital Wallet if restrictions apply to the Card or if the risk parameters of the security systems or the rules of the payment systems are not met.

6. RIGHTS AND OBLIGATIONS OF THE PARTIES

6.1. The Bank may:

6.1.1. Refuse to provide Services to the User or suspend the Transaction in case of detection of signs of questionable transactions, fraud or breaches of the laws of the Republic of Uzbekistan (including AML/CFT requirements).

6.1.2. Set and unilaterally change limits on the amount and number of Transactions, as well as the list of available Services and RSOs in the Mobile Application.

6.1.3. Withhold the Commission for the provided Services in accordance with the Tariffs without acceptance.

6.1.4. Temporarily suspend the operation of the Mobile Application for scheduled technical or preventive maintenance, notifying Users about it in available ways.

6.1.5. Request additional information or documents from the User confirming the legality of the Transactions performed or the User's identity.

6.1.6. Make a request to debit funds from the Client's accounts attached to Third-Party Bank Cards added by the User to the Mobile Application. The User hereby grants the Bank the unconditional right to send such requests to Third-Party Banks in order to execute the User's Orders.

6.1.7. Execute no User's orders received by the Bank via the Mobile Application until the circumstances are clarified, in case of:

— improper fulfillment by the User of obligations under the Agreement;

— detection or suspicion by the Bank about the illegality of Transactions carried out using the User's Card and/or Accounts;

— identification by the Bank of the Client's Transactions that, in accordance with the laws of the Republic of Uzbekistan, contain questionable Transactions related to the legalization of proceeds from criminal activities, financing of terrorism and financing the proliferation of weapons of mass destruction, or Transactions that violate the applicable laws of the Republic of Uzbekistan.

6.1.8. Refuse to add a Card to a Digital Wallet or unilaterally block, suspend, or delete a created Token if data compromise is suspected, signs of fraudulent transactions are detected, security requirements are breached, or the relevant payment system or Digital Wallet operator so requests.

6.2. The Bank shall:

6.2.1. Process the User's orders in a timely and high-quality manner, provided that they comply with all the terms of the Offer.

6.2.2. Ensure the protection of the User's personal data and to observe the banking secrecy of Transactions.

6.2.3. Promptly publish information about changes in the Offer or Tariffs on the Bank's Website and/or in the Mobile Application.

6.2.4. Inform the User about detected signs of fraud, information security, cybersecurity, and fraud incidents through available communication channels.

6.3. The User may:

6.3.1. Use the functionality of the Mobile Application to perform Transactions 24/7, except during scheduled maintenance or repair.

6.3.2. Link Third-Party Bank Cards for Transactions via the Mobile Application.

6.3.3. Receive up-to-date information about Tariffs, limits, and the status of your Transactions through the Bank's Website and/or Mobile Application.

6.3.4. Stop using the Mobile Application at any time by performing a technical action to delete the Personal Account in the interface of the Mobile Application. This action of the User is recognized as the initiation of termination of the Agreement, provided that the User has no debt to the Bank and completes all previously initiated Transactions.

6.4. The User shall:

6.4.1. Transfer no Authentication Data, Verification Codes, and Mobile Device to third parties. Ensure the safety of data for access to the Personal Account. Not to register any third party’s biometric data in the operating system of a Mobile Device on which the Mobile Application is used and/or a Digital Wallet linked to Cards issued by the Bank is configured.

6.4.2. Provide the Bank with reliable information and timely (no later than 1 (one) day) notify of a change in the mobile phone number or loss of access to it.

6.4.3. Use only official (licensed) software, update the Mobile Application in a timely manner, and use antivirus tools.

6.4.4. Do not use the Mobile Application to carry out illegal business activities, as well as Transactions related to the legalization of proceeds from criminal activities, the

financing of terrorism and the financing of the proliferation of weapons of mass destruction.

6.4.5. Carefully read the notifications sent by the Bank, including PUSH notifications in the mobile application, SMS notifications regarding detected signs of fraud, information security, cybersecurity, and fraud incidents,

— Take into account the information provided by the Bank about detected signs of fraud and exercise increased caution when confirming any payment transactions after receiving these notifications;

— immediately, but no later than 1 (one) day after the fact is revealed, notify the Bank of the loss (theft) of the device with which access to banking services is carried out, or of taking control over such device by third parties;

— notify the Bank of the transaction without its consent within 1 (one) day from the moment of detection of such fact;

— provide the Bank with the contact information necessary for communication, in case of their change, within 3 (three) days from the date of such changes;

— at the request of the Bank, the User undertakes to provide information that the transaction was carried out thereby independently or performed by a third party on its behalf or voluntary consent;

— provide the Bank with information about fraud cases.

6.4.6. Take extra care when scanning QR codes posted in public places. The User independently bears the risk of making a payment using forged or altered QR codes if the data in the Payment Window (name of the RSO and amount) has not been verified by the User before confirming the Transaction.

7. RESPONSIBILITY OF THE PARTIES

7.1. The Parties are responsible for non-fulfillment or improper fulfillment of their obligations under this Agreement in accordance with the legislation of the Republic of Uzbekistan and the terms of the Offer.

7.2. The Bank is not responsible for Transactions made by third parties using the User's Authentication Data (either with or without its knowledge), except in cases where the Bank's direct fault in the leakage of such data is proven.

7.3. The Bank is not responsible for failures in the operation of the Internet, communication channels, power supply, as well as for technical errors on the part of payment systems and correspondent banks.

7.4. The Bank is not responsible for the consequences of executing the User's Order if it contains erroneous details of the recipient (card number, account, amount, etc.). The responsibility for the correctness of the data in the Payment Window lies entirely with the User.

7.5. The Bank shall not be liable for any loss resulting from the User’s Mobile Device being infected with viruses or malicious software, or from the use of modified operating systems that violate security standards. The Bank shall also not be liable for any failures, delays, or malfunctions of Digital Wallets caused by faults in the Mobile Device’s operating system or third parties’ server infrastructure.

7.6. The Bank is not responsible for the refusal of a Third-Party Bank to execute a request for funds withdrawal, as well as for additional fees and restrictions set by a Third-Party Bank when making Transactions through the Mobile Application.

7.7. The User is solely responsible for the safety of its Mobile Device, SIM card, as well as Authentication Data and Verification Codes. All actions performed in the Personal Account after successful authorization are recognized as committed by the User itself.

7.8. The User bears the risk of losses incurred as a result of late notification to the Bank about the loss of the Mobile Device or compromise of its personal data.

7.9. The User is responsible for any Transactions that have been recognized as authorized (confirmed by a Verification Code or Biometrics), even if they were committed under the influence of fraudulent actions by third parties.

7.10. The Parties are released from liability for partial or complete non-fulfillment of obligations under the Agreement if it was the result of force majeure, including, but not limited to: natural disasters, military actions, acts of government agencies, major accidents on main communication channels.

7.11. In any case, the amount of the Bank's liability is limited by the amount of the Commission actually paid for this Transaction. The Bank does not compensate the User for indirect losses or lost profits.

7.12. The Bank shall ensure that a secure Tokenization request is generated and transmitted from the Mobile Application to the Digital Wallet. The Bank shall not be liable for the subsequent processing or storage of the Token by the Device's hardware modules, or for any refusal by retail or service establishments to accept payments made using the Digital Wallet.

8. PROTECTIVE ACTIONS AGAINST UNAUTHORIZED TRANSACTIONS

8.1. A transaction is considered authorized if the order for its execution is confirmed using the User's Authentication Data (Verification Code, Biometrics, PIN, etc.), and the Bank has not found violations of the established procedure for protective actions during verification.

8.2. In case of loss of the Mobile Device, SIM card, or if there is a suspicion that Authentication Data has become known to third parties, the User shall immediately (no later than 1 (one) hour from the moment of discovery) contact the Bank's Contact Center or block access to the Personal Account independently (if technically possible).

8.3. Until the Bank receives notification of the loss/compromise, the risk of losses on all Transactions made using the User's identification funds is borne by the User.

8.4. The Bank has the right to suspend the Transaction or block access to the Mobile Application if the Transaction parameters correspond to the signs of making a payment without the User's consent.

8.5. In case of blocking, the Bank informs the User in available ways to confirm or deny the legitimacy of the Transaction.

8.6. The Bank conducts an internal audit of an unauthorized Transaction within the time limits defined by the laws of the Republic of Uzbekistan.

8.7. The Bank has the right to refuse to refund amounts for unauthorized Transactions if it is established that they became possible due to:

8.7.1. fraudulent actions of the User;

8.7.2. transfer of verification codes or devices by the User to third parties;

8.7.3. failure by the User to comply with the security measures described in this Offer.

8.8. The User is solely responsible for any Transactions confirmed using Face ID or Touch ID, if biometric data of third parties is stored in the settings of the User's Mobile Device. The Bank shall not verify whose face or fingerprint (of the User or a third party) was used to confirm the Transaction, if the authentication was successfully recognized by the device's operating system.

9. DISPUTE RESOLUTION

9.1. All disputes and disagreements arising out of or in connection with this Offer will be resolved by negotiation between the Parties.

9.2. The Parties recognize the electronic protocols (logs) of the Bank's software and payment systems as appropriate and sufficient evidence.

9.3. The Parties acknowledge that electronic documents generated using the User's Authentication Data in the Mobile Application have the legal force of handwritten documents and are sufficient confirmation of the User's will.

9.4. If it is impossible to resolve disputes through negotiations, the dispute shall be considered in court at the Bank's location (legal address) in accordance with the applicable laws of the Republic of Uzbekistan.

9.5. This Offer and the relations of the Parties are regulated by the applicable laws of the Republic of Uzbekistan.

10. VALIDITY, AMENDMENT AND REVOCATION

10.1. This Offer comes into force from the date of its Acceptance by the User in accordance with the procedure provided for in the section 3 of this Offer, and is valid until the termination of the obligations of the Parties on the grounds provided for by this Agreement or the laws of the Republic of Uzbekistan.

10.2. Procedure for making changes:

10.2.1. The Bank has the right to unilaterally make changes and/or additions to the terms of this Offer and the Bank's Tariffs.

10.2.2. The Bank shall notify the User of changes in the terms of the Offer and Tariffs at least 10 (ten) calendar days prior to the effective date of such changes.

10.2.3. The notification is made by posting a new version of the Offer/Rates on the Bank's Website and in the Mobile Application. Additionally, the Bank may send a PUSH notification or message to the Personal Account.

10.2.4. If the User does not agree with the proposed changes, it may terminate the Agreement unilaterally before the effective date of the changes by deleting its Personal Account in accordance with the procedure provided for in the Offer.

10.2.5. If the User has not deleted his Personal Account before the effective date of the changes and continues to use the Mobile Application (i n particular, performing any Transaction or authorization after the changes take effect), such changes are considered fully accepted by the User.

10.3. Revocation of the Offer:

10.3.1. The Bank may prematurely withdraw this Offer (terminate it) at any time due to technical, organizational, legal or other reasons.

10.3.2. The Bank notifies the User about the withdrawal of the Offer by sending a message to its Personal Account or posting information on the Bank's Website indicating the reasons for the withdrawal.

10.4. Termination of the Agreement:

10.4.1. The Agreement may be terminated at the User's initiative at any time. To terminate the contractual relationship, the User shall delete its Personal Account directly in the interface of the Mobile Application.

10.4.2. The Parties acknowledge and confirm that deleting (uninstalling) the Mobile Application from the User's device is not an action aimed at terminating the Agreement and does not terminate the obligations of the Parties.

10.4.3. Termination of the Agreement by deleting the Personal Account is possible only if the User has no debt to the Bank and all current (initiated) Transactions are completed.

10.4.4. The Bank may terminate the Agreement unilaterally in the event of a systematic breach by the User of the terms of the Offer or in cases provided for by the laws of the Republic of Uzbekistan, in particular, AML/CFT.

10.5. All changes and additions to this Offer from the effective date apply to all Users, including those who accepted the Offer before the effective date.

11. CONFIDENTIALITY AND DATA PROCESSING

11.1. In accordance with the Laws of the Republic of Uzbekistan On Personal Data, On Banking Secrecy and On Informatization, the User, by accepting this Offer, gives his full and unconditional consent to the Bank for the collection, systematization, accumulation, storage, use, processing, cross-border transfer, destruction and provision of access to personal data and information that constitutes a banking secret.

11.2. Consent is provided for the purposes of fulfilling obligations under this Offer, identification (including biometric identification), providing banking and payment services, providing information about the Bank's products, as well as complying with AML/CFT laws.

11.3. The consent applies to all information received by the Bank during the service process.

11.4. Data processing and storage period:

11.4.1. The Bank processes and stores the User's personal data during the entire term of this Agreement.

11.4.2. After the termination of the Agreement and the deletion of the Personal Account, the Bank shall ensure the storage of personal data and information about the User's Transactions for the period defined by the laws of the Republic of Uzbekistan.

11.4.3. Upon expiration of the established retention periods, the Bank undertakes to destroy or depersonalize the User's personal data, unless otherwise provided by law.

11.5. The User grants the Bank the right to receive, transfer and process its personal data in the information systems of authorized government agencies, payment organizations, processing centers and credit bureaus necessary for identity verification and financial transactions.

11.6. The User consents to the use of its data from centralized databases (including databases of tax authorities, depositor systems and biometric identification systems, etc.) integrated with the Bank's information systems.

11.7. The provision of recipient's data by the User for the purpose of performing a Transaction is recognized as an action performed in the interests of the User and recipient, and is not considered disclosure of confidential information or violation of the rules of personal data processing by the Bank.

11.8. By accepting the Offer, the User agrees to receive from the Bank advertising, informational and commercial messages (SMS, Push notifications, E-mail) related to the services of the Bank and its partners.

11.9. The Parties recognize the documents generated in the Mobile Application as equivalent to paper documents signed by hand in simple written form.

12. FORCE MAJEURE CIRCUMSTANCES

12.1. The Parties are released from liability for partial or complete non-fulfillment of their obligations under this Offer if it resulted from force majeure circumstances that arose after the conclusion of the Agreement as a result of extraordinary events that the Parties could not have foreseen or prevented by reasonable measures.

12.2. Force majeure circumstances include:

12.2.1. Natural disasters (earthquakes, floods, fires, epidemics/pandemics);

12.2.2. Socio-political events (military actions, terrorist acts, strikes, civil unrest);

12.2.3. State legal acts (adoption by state authorities, management bodies or the Central Bank of the Republic of Uzbekistan of acts or measures of a restrictive and prohibitive nature, including sanction restrictions);

12.2.4. Technological factors that arose through no fault of the Bank, but affect the fulfillment of obligations: system failures in the software of payment systems, global failures in the Internet, power supply or backbone data transmission systems.

12.3. The Party for whom it is impossible to fulfill its obligations shall notify the other Party within 3 (three) business days after such circumstances occur (when it became aware of the occurrence).

12.3.1. The Bank notifies the User by posting information on the official website or through communication channels (PUSH/SMS).

12.3.2. The User notifies the Bank by personal appearance or through official communication channels.

12.4. The fact of force majeure circumstances shall be documented by the relevant authorized state bodies or organizations of the Republic of Uzbekistan.

12.5. Late notification of force majeure deprives the Party of the right to refer to them as a basis for exemption from liability, except in cases where the circumstance itself prevented such notification.

12.6. The period for fulfilling obligations under the Agreement is postponed in proportion to the time during which the force majeure circumstances and their consequences were in effect. If the specified circumstances last more than 30 (thirty) calendar days, the Parties have the right to terminate the Agreement by making full settlements on the date of termination.

13. ANTI-CORRUPTION CLAUSE

13.1. The Parties recognize and confirm that they pursue a zero tolerance policy towards corruption and other manifestations of corruption. The Parties undertake to comply with the requirements of the laws of the Republic of Uzbekistan on combating corruption, as well as the applicable norms of international law.

13.2. In fulfilling their obligations under this Agreement, the Parties, their affiliates, employees, or intermediaries undertake not to commit (offer, promise, or authorize) actions that qualify as:

13.2.1. Giving or receiving a bribe;

13.2.2. Mediation in bribery;

13.2.3. Commercial bribery;

13.2.4. Abuse of official position or other actions that breach the requirements of anti-corruption laws in order to obtain undue advantages.

13.3. If one of the Parties suspects that any anti-corruption provisions have been breached or may be breached, the relevant Party undertakes to notify the other Party in writing or through the communication channels within 3 (three) business days.

13.4. The Bank has the right to request additional documents and explanations on Transactions from the User if the nature of such Transactions gives reason to believe that there is a corruption component or other illegal purposes.

13.5. Consequences of the breach:

13.5.1. A breach of the User's anti-corruption obligations, documented or identified during an internal audit of the Bank (compliance control), is a significant breach of the terms of the Agreement.

13.5.2. In case of breaches, the Bank has the right to unilaterally suspend the service, block access to the Mobile Application, or terminate the Agreement completely.

13.5.3. The Party guilty of breaching the anti-corruption conditions shall compensate the other Party for the losses incurred as a result of such breach.

13.6. The Bank is not responsible for any negative consequences (losses, fines) incurred by the User in connection with the lawful application by the Bank of the measures provided for in this section.

14. FINAL PROVISIONS

14.1. This Offer is provided to the User in the language selected by him in the interface settings of the Mobile Application from the list of available languages.

14.2. All language versions of the Offer have the same legal force. In case of discrepancies in the interpretation of the terms, the version in the language in which the actual Acceptance of the Offer was made by the User shall take priority.

14.3. If any of the provisions of this Offer are declared invalid or unenforceable by the court (including due to changes in legislation), this does not invalidate the entire Offer as a whole.

14.4. The invalid provision of the Offer shall be replaced with a new one that best meets the terms of the Offer. The remaining provisions remain in full force and effect.

14.5. All notifications and documents sent by the Bank to the User via the Mobile Application are considered delivered and received at the time of their sending.

14.6. The User independently bears the risks associated with untimely familiarization with the information in his Personal Account or changing the notification settings on his Mobile device.

14.7. In case of a change in the legal address, bank details or contact details of the Bank, the relevant information is posted on the Bank's website, which is recognized as a proper notification.

14.8. In everything that is not directly regulated by this Offer, the Parties shall be guided by the applicable laws of the Republic of Uzbekistan, the rules of payment systems and internal regulations of the Bank.

15. BANK DETAILS

Octobank JSC
Legal address: 2 Furkat Street, Tashkent, 100021, Republic of Uzbekistan.
TIN: 203644820
NCEA: 64190
Bank code: 00980
Settlement account: 29802000700000980110
Website: www.octobank.uz
Phone: (+998) 71 202-33-33
E-mail: info@octobank.uz

Appendix No. 1 to the Public Offer
On Provision of Payment Services through
the Octomobile Mobile Application

COMPLIANCE CONDITIONS

1. PURPOSE AND DEFINITIONS

1.1. The purpose of these Terms of Compliance (the "Terms") is to prevent the risks associated with compliance with the laws and international standards for the Client arising in the areas of:

- "Combating money laundering, terrorist financing and financing the proliferation of weapons of mass destruction" ("AML/CFT/FRMU/FPWMD");
- "Combating bribery and corruption" (CB&C);
- Sanctions and export control measures.

Money laundering shall mean legitimization of the possession, use, or disposal of funds or other property obtained as a result of a crime.
Terrorist financing shall mean provision of funds or financial support to terrorists.
Corruption shall mean illegal use of an official position to gain benefits.
Bribery shall mean transfer, promise, or authorization of receiving a bribe for illegal influence.
Sanctions shall mean financial and property restrictions, economic and trade measures imposed by government agencies.
Sanctions list shall mean a list of individuals and/or legal entities, countries, goods and services subject to sanctions.
Export control shall mean laws and regulations governing the import, export, and transfer of goods, technologies, and services.
Bank shall mean Octobank Joint Stock Company, which is a financial institution providing banking services, including cash transactions and lending.
Client shall mean an individual who has entered into a contractual relationship with the Bank and undertakes to comply with these Terms.

2. LEGAL BASIS

2.1. As part of these Terms, the client undertakes to comply with the laws of the Republic of Uzbekistan and international standards.

2.2. The following documents are not limited to local requirements:

- Criminal Code of the Republic of Uzbekistan;
- Law On Combating Corruption;
- Law On Combating the Legalization of Proceeds of Crime and the Financing of Terrorism;
- Client's procedures in the field of AML/CFT/CFMEU/FPWMD, CB&C and sanctions.

2.3. International standards include:

- FATF recommendations on combating money laundering;
- ISO 37001:2025 — Anti-corruption system standard;
- Sanctions lists of the UN Security Council, the EU, OFAC, the UK and other bodies.

3. INTERNATIONAL SANCTIONS

3.1. International sanctions shall mean financial and material restrictive measures, economic and trade restrictions imposed or applied by international organizations such as the United Nations, the EU, the United States, the United Kingdom and others.

3.2. For the purposes of these Terms, a person subject to restrictive measures" shall mean a legal entity or individual subject to international sanctions.

3.3. The Client undertakes not to provide goods, services or financing that may violate international sanctions.

4. CLIENT'S RESPONSIBILITIES

4.1. The Client undertakes to comply with the laws of the Republic of Uzbekistan and the international standards specified in paragraphs 2 and 3, in particular:

- not to engage in money laundering
- not to engage in terrorist financing;
- not to contribute to financing the proliferation of weapons of mass destruction;
- not to engage in financial fraud;
- not to provide bribes to employees or third parties;
- not to enter into transactions with sanctioned clients;
- ensure full and transparent provision of documents on transactions and goods.

4.2. The Client releases the Bank from liability for any losses, costs or penalties related to the breach of these terms.

5. BANK'S RIGHTS

5.1. If the Client breaches the terms of these Terms, the Bank has the right to unilaterally terminate contractual relations with the Client without any liability.

5.2. If there is a risk of sanctions being applied to the Bank, it may refuse to conclude a contract or conduct operations.